EXHIBIT 44

Disconnect - Tracker Protection lists

DISCONNECT.

Consumer   Enterprise

We track the trackers

Disconnect - Tracker Protection lists

Tracking protection lists

Our tracker protection lists are created by scanning and mapping network requests found in millions of websites, apps, and emails. We then utilize AI and other methods to analyze the dataset and identify potential "trackers" defined according to our policy. Potential trackers are then processed for both technical and policy review. Positive results are subject to compatibility tests and categorized as described below.

- Definition of tracking
- Trackers we block
- Trackers we don't block
- Categories of trackers
- Submissions and appeals

Definition of Tracking

Tracking is the collection of data regarding a particular user's or device's activity across multiple websites or applications that aren't owned by the data collector, and the retention, use or sharing of that data. We will also classify as trackers domains which collect, share, retain, or use data to enable tracking by other services.

Our definition focuses on third-party data collection AND retention. So, for example, our tracker definition doesn't apply to sites that log an IP address but don't save that information in a database. And the collection must be across context, so our tracker definition also doesn't apply to cases where there is solely a first-party relationship with the user, for example the site only collects and retains information on site visitors. Finally, our definition also focuses on particular users and devices, so data that is immediately aggregated doesn't apply.

Trackers we block

"Trackers" are those services that we've identified and determined meet the definition of tracking above.

Disconnect compiles several lists of trackers for browsers, apps, full device, and network based protection. The list of trackers that power our browser extensions and are utilized by Mozilla's Firefox, Microsoft's Edge, and other browsers can be found here, along with a change log and notes. Example changes to this tracker list can be seen below.

| 12/27/2022 | Adds more verified trackers |
| 10/31/2022 | Adds more verified email trackers |

Trackers we don't block

Disconnect strives to find the balance between privacy, security, usability and promoting a better Internet for everyone. These concerns drive our decisions in regards to trackers we block and don't block. We do not accept payment for unblocking trackers.

We unblock trackers to provide a better user experience, based on the three types of evidence listed below. These unblocked trackers will appear in what we call the Content portion of our list. For some of our products and services, users can choose to block this portion of the list as well.

* Error reporting. We sometimes unblock trackers based on user feedback and complaints that we have received about broken user experiences or compatibility issues.

10/15/23, 6:22 PM

Disconnect - Tracker Protection lists

* **Internal testing**. We conduct compatibility and us testing of our list to identify domains that should go on our unblocked list.

* **User experiments**. We also use external testing services to run user experiments and identify additional problems with our products and tracking list.

We also generally unblock tracking domains that require users to transparently and explicitly opt in to data collection and retention on every third-party website and app in which the tracker domain appears.

Although we support sites that commit to respect users' Do Not Track (DNT) preferences and agree to comply with DNT as defined by the Electronic Frontier Foundation (https://www.eff.org/dnt-policy) such compliance is not grounds for unblocking at this time due to disparities and technical inability to persist DNT headers across browsers and products.

All of the trackers we've identified but don't block in our browser based lists, along with a change log and notes, can be found here.

| 12/1/2022 | my.mail.ru Adds my.mail.ru to Content section |
| 7/27/2022 | Moving verified chatbot trackers from Content to Analytics |

Categories of trackers

Our lists of trackers are categorized according to the following definitions.

Advertising: A tracker which also displays or enables ads or marketing offers. These types of ads can track your personal information and expose you to malware, even if you don't interact with them.

Disconnect - Tracker Protection lists

Analytics: A tracker which collects your information and may build a profile based on your online activity that can be connected with your real name or other unique identifier.

Anti-fraud: A tracker may be classified as anti-fraud if its explicit purpose is to prevent or detect fraud and does not utilize data collected in a third-party context (including IP addresses and user identifiers) for any purpose not directly related to fraud detection or prevention, including the use and sharing of such data to enable tracking of particular users or devices by other services.

Cryptomining: A domain may be classified as cryptomining if it can cause the user's browser to mine cryptocurrencies without explicit user opt-in.

Email: A tracker which commonly appears in emails. In addition to the main Email category, we will maintain a sub-category called Email Aggressive. This sub-category includes additional email tracker domains which serve images or links that when blocked may alter expected functionality. Determinations about whether a domain is moved to the Email Aggressive category seek to balance usability with privacy harm and will be based on error reporting, internal testing, and user experiments as described in the Content portion of our list above.

Fingerprinting: A tracker may be classified as a fingerprinter if it identifies particular users or devices based on the properties of the browser, device, network, or any other properties of the computing environment, without using client-side storage of cookies or other data.

We differentiate between two sub-categories of fingerprinters:

- A tracker may be classified as a general fingerprinter if it uses browser or device features or properties in unintended ways to identify and track a particular user or device.

- A tracker may be classified as an invasive fingerprinter if it uses an API to extract information about a particular user's computing environment when the API was not designed to expose such information.

Session replay: A tracker which records all actions a user takes on a webpage in order to recreate the user's session may be classified as a replay script.

Social: A tracker may be classified as social if it uses tracking techniques that allow a social networking service to track your web browsing activities even when you are not on the social network's website or app.

Submissions and appeals

Our tracker protection lists are dynamic and we welcome and rely on feedback from our community. If you believe that we've missed a tracker, or categorized a domain incorrectly please fill out and submit the form below.

Please note, classifications are based on technical analysis and review of publicly available, legally binding policies and statements.

Every appeal or submission should include the domain(s) at issue and a proposed rationale for adding, removing, or re-categorizing the domain(s) based on Disconnect's policies and definitions. Optionally, a description of where a domain was observed in a third-party context, additional notes, and a contact email may be submitted in case follow up beyond the published issue is necessary.

10/15/23, 6:22 PM

Disconnect - Tracker Protection lists

Domain(s) to review: (Separate them by comma)

Rationale for removing, adding, or recategorizing:

Where domain(s) observed: (Separate them by comma)   Optional

Additional notes: Optional

Contact email: Optional

john@example.com

Submit

COMPANY

About

Announcements

Privacy

CONSUMER

Premium

Pro

Basic

BUSINESS

Network

Apps

Education

10/15/23, 6:22 PM

Disconnect - Tracker Protection lists

Terms

Privacy DNS

FAQ

DNT

© 2023 Disconnect.